Amendments to the Drawings:

The attached replacement sheets of drawings include changes to FIGs. 3 and 4, and replaces the original sheets including FIGs. 3 and 4.

FIGs. 3 and 4 have been amended to correspond with the specification, and to reflect that a pseudo-random number is generated in response to hashing a pass phrase from a user, as recognized by the Examiner. No new matter has been added.

Replacement Sheets (2 pages)

REMARKS

Please cancel claims 1-30 without prejudice, as Applicant reserves the right to pursue the cancelled claims in a continuation application. Claims 31-50 are newly submitted. The specification has been amended to correct informalities. The drawings have been amended to correct informalities and to correspond with the specification. No new matter has been added. Accordingly, claims 31-50 remain pending in the application. Reconsideration is respectfully requested in view of the amendments to the claims and the remarks below.

I. The § 112 Rejections

Claims 3, 7, 18, 22 and 24 were rejected under 35 U.S.C. § 112, second paragraph, ass being indefinite. In particular, the Examiner pointed out that hashing a pass phrase will result in a pseudo-random number, and such should be indicated in the claims. Applicant would like to thank the Examiner for recognizing the error. Accordingly, Applicant has provided recitation of the pseudo-random number in the claims presented above.

II. The § 103 Rejections

Claims 1-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,850,443 ("Oorschot") in view of U.S. Patent No. 6,061,799 ("Eldridge").

Applicant respectfully traverses the rejections.

Claim 31 recites a method for securely storing a key using a secure chip associated with a computer system. The method includes creating a migratable keyblob. The migratable keyblob contains a key having been encrypted based at least in part on use of a first random number. The method further includes receiving user input creating a pass phrase to encrypt the first random number, and encrypting the first random number using the pass phrase to prevent unauthorized

usage of the first random number to decrypt and recover the key contained in the migratable keyblob.

A. Oorschot Fails To Disclose Encrypting a First Random Number Using a Pass Phrase to Prevent Unauthorized Usage of the First Random Number to Decrypt and Recover a Key Contained in a Migratable Keyblob

Oorschot discloses a key management system for mixed-trust environments, and methods for transporting a symmetric key encrypted with an asymmetric encryption technique (see Abstract). In particular, with reference to FIG. 1, Oorschot discloses creating a (high-trust) symmetric key "K", and separately encrypting the symmetric key "K" with a public-key of each intended recipient. The copies of the encrypted symmetric key "K" are then placed in corresponding header fields (col. 5, line 60 – col. 6, line 6).

Oorschot, however, fails to disclose encrypting a first random number using a pass phrase to prevent unauthorized usage of the first random number to decrypt and recover a key contained in a migratable keyblob. According to Applicant's invention, a key is encrypted using a first random number. The first random number is then further encrypted with a pass phrase received from a user. In contrast, the symmetric key of Oorschot is encrypted using a public key of an intended recipient. Even assuming, *arguendo*, that the public key to be a random number (which Applicant does not concede), Oorschot fails to disclose further encrypting the public key with a pass phrase received from a user. The Examiner recognizes that Oorschot fails to disclose encrypting a first random number using a pass phrase. The Examiner, however, asserts that these limitations, as well as further limitations absent from Oorschot and recited in claim 1, are disclosed by Eldridge.

B. Eldridge Fails To Disclose Encrypting a First Random Number Using a Pass Phrase to Prevent Unauthorized Usage of the First Random Number to Decrypt and Recover a Key Contained in a Migratable Keyblob

Eldridge discloses removable media for password based authentication in a distributed system (see Abstract). Specifically, Eldridge discloses concatenating a secret parameter 302 and a current password 304, and supplying the result to a pseudo-random number generator 320. The output of the pseudo-random number generator 320 represents a public/private key that can be used to encrypt and decrypt data (col. 5, line 56 – col. 6, line 8; FIG. 3B). The public/private key is used during authentication of a client process to a server process (col. 7, ll. 18-63).

Eldridge, however, fails to disclose encrypting a first random number using a pass phrase to prevent unauthorized usage of the first random number to decrypt and recover a key contained in a migratable keyblob. As discussed above, Eldridge discloses concatenating a secret parameter 302 and a current password 304. Even assuming, *arguendo*, that the secret parameter 302 is a random number (which Applicant does not concede), Eldridge fails to disclose that the secret parameter 302 is used to decrypt and recover a key contained in a migratable keyblob, as is required in claim 1. Instead, the secret parameter 302 is used to generate a public/private key pair.

Applicant respectfully submits that claim 31, and the claims that depend therefrom, are allowable over the references cited above.

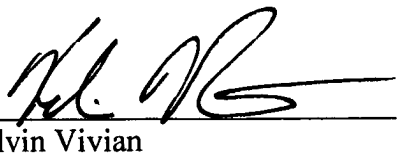
C. Other Independent Claims

Claims 39 and 47 each incorporates limitations similar to those of claim 31. Claims 39 and 47 (and the claims that depend therefrom) are also allowable over the references cited above for reasons corresponding to those set forth with respect to claim 31.

Applicant submits that claims 31-50 are allowable over the references cited above, and are in condition for allowance. Should any unresolved issues remain, the Examiner is invited to call the undersigned at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

May 15, 2006
Date



Kelvin Vivian
Attorney for Applicant(s)
Reg. No. 53,727
(650) 475-1448